
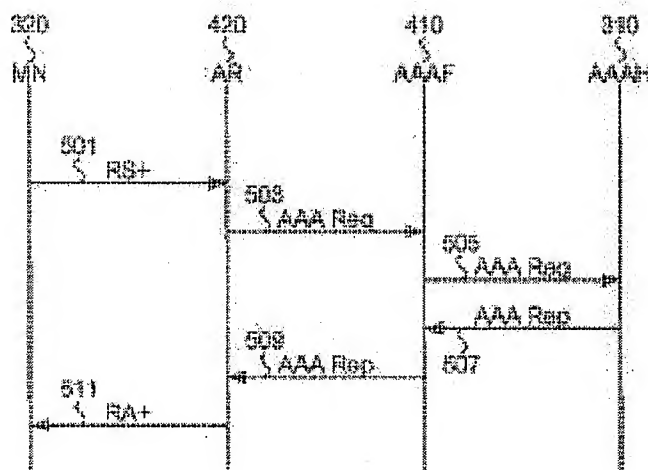


SECURE NETWORK ACCESS METHOD**Publication number:** JP2003218954 (A)**Publication date:** 2003-07-31**Inventor(s):** YEGIN ALPER E; HE XIAONING; WILLIAMS CARL**Applicant(s):** DOCOMO COMM LAB USA INC**Classification:**

- international: G09C1/00; H04L9/32; H04L12/28; H04L12/66; H04Q7/22; H04Q7/24; H04Q7/26; H04Q7/30; G09C1/00; H04L9/32; H04L12/28; H04L12/66; H04Q7/22; H04Q7/24; H04Q7/26; H04Q7/30; (IPC1-7): H04L12/66; G09C1/00; H04L9/32; H04L12/28; H04Q7/22; H04Q7/24; H04Q7/26; H04Q7/30

- European:**Application number:** JP20020324920 20021108**Priority number(s):** US20010345967P 20011109; US20020185359 20020628**Also published as:** JP3822555 (B2)**Abstract of JP 2003218954 (A)**

PROBLEM TO BE SOLVED: To provide a network-layer authentication protocols for authenticating mobile client and access router to each other.



Data supplied from the **esp@cenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2003-218954
(P2003-218954A)

(43) 公開日 平成15年7月31日 (2003.7.31)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード* (参考)
H 0 4 L 12/66		H 0 4 L 12/66	E 5 J 1 0 4
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 E 5 K 0 3 0
H 0 4 L 9/32		H 0 4 L 12/28	3 0 3 5 K 0 3 3
12/28	3 0 3	9/00	6 7 5 Z 5 K 0 6 7
H 0 4 Q 7/22		H 0 4 Q 7/04	A

審査請求 有 請求項の数37 O L (全 20 頁) 最終頁に続く

(21) 出願番号 特願2002-324920 (P2002-324920)

(22) 出願日 平成14年11月8日 (2002.11.8)

(31) 優先権主張番号 6 0 / 3 4 5 9 6 7

(32) 優先日 平成13年11月9日 (2001.11.9)

(33) 優先権主張国 米国 (US)

(31) 優先権主張番号 1 0 / 1 8 5 3 5 9

(32) 優先日 平成14年6月28日 (2002.6.28)

(33) 優先権主張国 米国 (US)

(71) 出願人 301077091

ドコモ コミュニケーションズ ラボラ
トリーズ ユー・エス・エー インコーポレ
ーティッド
アメリカ合衆国, カリフォルニア州
95110, サンノゼ, スイート300, メトロ
ドライブ 181

(74) 代理人 100098084

弁理士 川▲崎▼ 研二 (外1名)

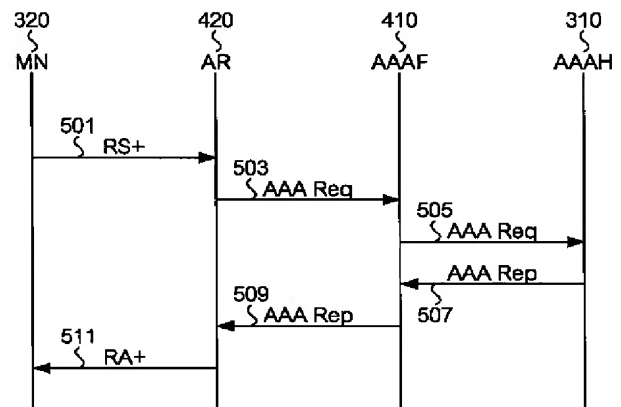
最終頁に続く

(54) 【発明の名称】 安全なネットワークアクセス方法

(57) 【要約】

【課題】 モバイルクライアントおよびアクセスルータを互いに認証するネットワーク層プロトコルを提供する。

【解決手段】 モバイルクライアント320は、請求メッセージ (RS+) を送信し、接続サービスを要求する。この請求メッセージ (RS+) は、モバイルクライアント320の身元証明書を含んでいる。この請求メッセージ (RS+) を受信したアクセスルータ420は、身元証明書が確認されるまでこの請求メッセージ (RS+) に対し応答しない。モバイルクライアント320の身元証明書が確認されてはじめて、アクセスルータ420は応答し、モバイルクライアント320に対し通知メッセージ (RA+) を返信する。従って、不正なモバイルクライアントのネットワークアクセスを防止できる。



【特許請求の範囲】

【請求項1】 モバイルクライアントが、自身の身元証明書を含む請求メッセージを送信する送信ステップと、信用できる実体が、前記身元証明書を確認する確認ステップと、前記身元証明書が正常に確認された場合のみ、アクセスルータが通知メッセージを返信する返信ステップと、を具備することを特徴とする認証過程。

【請求項2】 前記信用できる実体が、前記モバイルクライアントと前記信用できる実体との間に位置するあらゆる仲介物を、前記モバイルクライアントに対し認証することを特徴とする請求項1に記載の認証過程。

【請求項3】 各々少なくとも1の管理サーバにより管理され、各々少なくとも1のアクセスルータを備えた複数の管理ドメインを有する通信ネットワークにおいて、前記送信ステップ、前記確認ステップ、および前記返信ステップを行うことを特徴とする請求項1に記載の認証過程。

【請求項4】 前記信用できる実体が、前記モバイルクライアントが属するホームドメインを管理するサーバであることを特徴とする請求項3に記載の認証過程。

【請求項5】 前記信用できる実体が、前記モバイルクライアントが訪問するフォーリンドメインを管理するサーバであることを特徴とする請求項3に記載の認証過程。

【請求項6】 前記信用できる実体は、前記モバイルクライアントから前記請求メッセージを受信するアクセスルータであることを特徴とする請求項3に記載の認証過程。

【請求項7】 前記通知メッセージは、前記モバイルクライアントが前記アクセスルータを認証するための、前記アクセスルータの身元証明書を含むことを特徴とする請求項1に記載の認証過程。

【請求項8】 モビリティサービングノードが、前記アクセスルータの前記身元証明書を含む通知メッセージを自発的に送信するステップと、前記モバイルクライアントが、前記身元証明書を確認するステップと、前記モバイルクライアントが前記身元証明書を確認できない場合、前記送信ステップ、前記確認ステップ、および前記返信ステップを行うステップと、を具備することを特徴とする請求項1に記載の認証過程。

【請求項9】 前記モバイルクライアントが前記アクセスルータと通信中、前記送信ステップ、前記確認ステップ、および前記返信ステップを行い、前記モバイルクライアントに対し前記アクセスルータを再認証し、前記アクセスルータからの前記通知メッセージが、前記アクセスルータの前記身元証明書を含むことを特徴とする請求項1に記載の認証過程。

【請求項10】 前記モバイルクライアントと通信中に、前記アクセスルータは、前記送信ステップ、前記確認ステップ、および前記返信ステップの実行を開始するため有効期間の短い通知メッセージを送信し、前記アクセスルータに対し前記モバイルクライアントを再認証することを特徴とする請求項1に記載の認証過程。

【請求項11】 データ通信には、IPv4が用いられることを特徴とする請求項1に記載の認証過程。

【請求項12】 データ通信には、IPv6が用いられることを特徴とする請求項1に記載の認証過程。

【請求項13】 非対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項1に記載の認証過程。

【請求項14】 対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項1に記載の認証過程。

【請求項15】 少なくとも前記請求メッセージおよび前記通知メッセージのうちいずれか1は、チャレンジを含むことを特徴とする請求項1に記載の認証過程。

【請求項16】 モバイルクライアントの身元証明書を含む請求メッセージを送信する送信部と、アクセスルータから通知メッセージを受信する受信部と、を具備し、

前記身元証明書が正常に確認された場合のみ、前記モバイルクライアントは前記通知メッセージを受信することを特徴とするモバイルクライアント。

【請求項17】 前記通知メッセージは、前記アクセスルータの身元証明書を含み、前記モバイルクライアントは、前記身元証明書を確認する機能を有することを特徴とする請求項16に記載のモバイルクライアント。

【請求項18】 前記モバイルクライアントが前記アクセスルータと通信中、前記送信部は前記アクセスルータに対し前記請求メッセージを送信し、前記アクセスルータを再認証することを特徴とする請求項16に記載のモバイルクライアント。

【請求項19】 データ通信には、IPv4が用いられることを特徴とする請求項16に記載のモバイルクライアント。

【請求項20】 データ通信には、IPv6が用いられることを特徴とする請求項16に記載のモバイルクライアント。

【請求項21】 非対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項16に記載のモバイルクライアント。

【請求項22】 対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項16に記載のモバイルクライアント。

【請求項23】 少なくとも前記請求メッセージおよび

前記通知メッセージのうちいずれか1は、チャレンジを含むことを特徴とする請求項16に記載のモバイルクライアント。

【請求項24】 各々少なくとも1つの管理サーバにより管理され、各々少なくとも1つのアクセスルータを備えた複数の管理ドメインを有するAAAネットワークであって、

自身の身元証明書を含む請求メッセージを送信するモバイルクライアントと、

前記身元証明書を確認する信用できる実体と、

前記身元証明書が正常に確認された場合のみ、通知メッセージを返信するアクセスルータと、

を具備することを特徴とするAAAネットワーク。

【請求項25】 前記信用できる実体が、前記モバイルクライアントと前記信用できる実体との間に位置するあらゆる仲介物を、前記モバイルクライアントに対し認証することを特徴とする請求項24に記載のAAAネットワーク。

【請求項26】 前記信用できる実体が、前記モバイルクライアントが属するホームドメインを管理するサーバであることを特徴とする請求項24に記載のAAAネットワーク。

【請求項27】 前記信用できる実体が、前記モバイルクライアントが訪問するフォーリンドメインを管理するサーバであることを特徴とする請求項24に記載のAAAネットワーク。

【請求項28】 前記信用できる実体は、前記モバイルクライアントから前記請求メッセージを受信するアクセスルータであることを特徴とする請求項24に記載のAAAネットワーク。

【請求項29】 前記通知メッセージは、前記モバイルクライアントが前記アクセスルータを認証するための、前記アクセスルータの身元証明書を含むことを特徴とする請求項24に記載のAAAネットワーク。

【請求項30】 前記アクセスルータは、自身の身元証明書を含む通知メッセージを自発的に送信し、前記モバイルクライアントは前記身元証明書を確認できない場合、前記請求メッセージを送信することを特徴とする請求項24に記載のAAAネットワーク。

【請求項31】 前記アクセスルータと通信中、前記モバイルクライアントは前記請求メッセージを送信し、前記アクセスルータは、前記モバイルクライアントが前記アクセスルータを認証するための、自身の身元証明書を含む通知メッセージを送信することを特徴とする請求項24に記載のAAAネットワーク。

【請求項32】 前記モバイルクライアントと通信中に、前記アクセスルータは有効期間の短い通知メッセージを送信し、前記モバイルクライアントに前記請求メッセージを送信させることを特徴とする請求項24に記載のAAAネットワーク。

【請求項33】 データ通信には、IPv4が用いられることを特徴とする請求項24に記載のAAAネットワーク。

【請求項34】 データ通信には、IPv6が用いられることを特徴とする請求項24に記載のAAAネットワーク。

【請求項35】 非対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項24に記載のAAAネットワーク。

【請求項36】 対称鍵アルゴリズムを用いて、前記確認が行われることを特徴とする請求項24に記載のAAAネットワーク。

【請求項37】 少なくとも前記請求メッセージおよび前記通知メッセージのうちいずれか1は、チャレンジを含むことを特徴とする請求項24に記載のAAAネットワーク。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本出願は、2001年11月9日に提出された「ルータ検出およびAAAを用いた安全なネットワークアクセス (Secure Network Access Using Router Discovery and AAA)」と題する米国仮出願60/345、967に関して優先権を主張する。なお、この仮出願は、本明細書において参照として援用される。また、本出願では、2002年5月15日に提出された「モバイルIPネットワークへのアクセスを安全にする方法 (METHOD FOR SECURING ACCESS TO MOBILE IP NETWORK)」と題する米国出願10/146、548、および2001年11月9日に提出された「モバイルIP登録 (MOBILE IP REGISTRATION)」と題する米国仮出願60/332、396が、相互に参照される。なお、これらの出願は、本明細書において参照として援用される。本発明は、クライアントがネットワークにアクセスする接続サービスを要求する場合、およびルータがネットワーク接続を提供する場合に、クライアントおよびアクセスルータを相互に認証する双方向セキュリティプロトコルに関する。本発明にかかるセキュリティプロトコルは、AAA (Authentication (認証)、Authorization (認可) and Accounting (課金)) に基づき、その実行において、ルータ検出 (Router Discovery) がキャリアとして用いられる。

【0002】

【従来の技術】携帯電話機、PDA (personal digital assistant) 等の全世界的にルーティング可能なIP対応装置の普及とともに、公開アクセスIPネットワークが広く張りめぐらされてい

る。とりわけ、近年の携帯無線技術の進歩および携帯電話システムの成長率は、場所に拘束されない通信に対する、市場の巨大な需要を示している。無線通信の役割は、ごく数年前の従来の音声および呼び出しモバイル無線サービスを大幅に越えた。最近、ネットワークの世界標準規格に関する公認の機関である国際電気通信連合（ITU）は、国際移動通信規格（IMT-2000）を発表した。この標準規格では、携帯電話機、PDA、携帯型コンピュータ等の無線モバイルクライアントによる広範囲なモバイルアクセスを可能にするいわゆる第3世代（3G）ネットワークを提案している。この第3世代ネットワークでは、モバイルクライアント、または移動クライアントはネットワーク資源へのアクセスを維持しながら自由に移動し、接続ポイントのある基地局から別の基地局へ変更することができる。3Gネットワークには、リンク層（レイヤ2）におけるモビリティを提供するものがある。しかし、将来のネットワーク（いわゆる4G）は、IP層（レイヤ3）におけるモビリティを提供すると予想されている。

【0003】インターネットアーキテクチャの進化およびインターネットの円滑な運用に関わる、ネットワークの設計者、運用者、供給業者、研究者からなる国際団体であるインターネット技術特別調査委員会（IETF）は、IP層におけるモビリティ支援のための標準規格をいくつか提案している。これら提案された標準規格には、IETFのRFC2002（別名、モバイルIPバージョン4（IPv4））や「IPv6におけるモビリティ支援」と題された草案「draft-ietf-mobileip-ipv6-17」（別名、モバイルIPバージョン6）のようなモビリティ支援のための標準規格がある。この2つの標準規格は、本願明細書において参照として援用される。IPv4およびIPv6で定義されるプロトコル運用によると、クライアントは、ネットワーク資源へのアクセスを維持しながらネットワーク上を移動し、接続ポイントのあるアクセスルータから別のアクセスルータへ変更することが可能になる。通常、この処理は、「レイヤ3（L3）ハンドオフ」と呼ばれる。

【0004】L3ハンドオフ処理をおこなう目的は、登録処理をつうじて移動クライアントのパケットルーティング情報を更新することである。クライアントは、「ホームアドレス」により、常に指定することができる。ここで、「ホームアドレス」とは、ホームネットワーク上のアクセスルータ（ホームルータ）により割り当てられるIPアドレス、またはクライアント自身により選択されたIPアドレスのことである。しかしながら、クライアントがフォーリンネットワーク上にあってホームネットワークから離れている場合、クライアントには、現在のネットワークへの接続ポイントを示す気付けアドレスが設定される。この気付けアドレスは、フォーリンネッ

トワーク上のアクセスルータ（フォーリンルータ）のアドレスであり、ホームネットワークから離れて動作するクライアントは、この気付けアドレスをホームルータに登録する。そして、登録要求を受信したホームルータは、クライアント宛のパケットを途中で回収し、クライアントの気付けアドレスへ転送する。モバイルIPv6では、ホームネットワークから離れたクライアントは、ホームルータおよび通信中の相手先ノードに対し対応更新（binding update）を送信する。相手先ノードは、クライアントのようなモバイルクライアントであってもよいし、クライアントにデータを提供するサーバであってもよい。そして、対応更新を受信した相手先ノードは、ホームルータを介さずクライアントに対しパケットを直接転送する。

【0005】

【発明が解決しようとする課題】移動クライアントが、訪問したネットワークにおいてネットワーク接続を要求する場合、セキュリティ上の重大な問題が生じる。クライアントは、ネットワークアクセスが許可される前に、常に認証されなければならない。認証されないクライアントは、不正IDまたは盗難IDを用いて無料でネットワーク資源にアクセスしようとする不正利用者かもしれない。また、そのようなクライアントは、ネットワークの秩序ある運用を乱すためだけに、ネットワークアクセスを要求する悪意をもったノードかもしれない。同様に、クライアントは、自己にネットワーク接続を提供しているアクセスルータを認証したいと思うかもしれない。アクセスルータは、クライアントの通信を盗聴したり、どこかへ転送したり、ただ中断するだけの不正なルータかもしれない。現在、さまざまなアクセス技術で、数多くの認証メカニズムが実行、採用されている。例として、PPPおよび802.11ネットワークの認証がある。これらのネットワークを利用する場合、リンク層で認証メカニズムが提供されるため、その認証メカニズムの適用範囲が特定のアクセス技術に限られてしまう、という欠点があった。従って、アクセス技術を選ばない認証メカニズムの提供が求められている。

【0006】

【課題を解決するための手段】上記の事情に鑑み、本発明は、ネットワーク層における認証メカニズムを用いることにより、アクセス技術を選ばない安全なネットワークアクセス方法を提供する。本発明は、モバイルクライアントにネットワークアクセスを許可する前に、モバイルクライアントおよびアクセスルータを互いに認証するネットワーク層プロトコルを提供する。本発明は、ルータ検出をキャリアとして用い、認証プロトコルを実行する。本発明の実施形態において、モバイルクライアントは、請求メッセージを送信し、接続サービスを要求する。この請求メッセージは、モバイルクライアントの身元証明書を含んでいる。この請求メッセージを受信した

アクセスルータは、身元証明書が確認されるまでこの請求メッセージに対し応答しない。モバイルクライアントの身元証明書が確認されてはじめて、アクセスルータは応答し、モバイルクライアントに対し通知メッセージを返信する。従って、不正なモバイルクライアントのネットワークアクセスを防止できる。

【0007】アクセスルータからの通知メッセージは、アクセスルータの身元証明書を含んでいてもよい。このアクセスルータの身元証明書が正常に確認された場合のみ、モバイルクライアントは、このアクセスルータを介してネットワークアクセスを開始する。従って、モバイルクライアントが不正なアクセスルータを介してネットワークアクセスを開始してしまうことを防止できる。

【0008】請求および通知メッセージを用いることにより、ネットワークアクセスを安全にする上での利点が得られる。検出メカニズムは、モバイルクライアントとアクセスルータとがオフリンク接続を確立する際の第一歩である。すなわち、検出メカニズムを用いてモバイルクライアントおよびアクセスルータを認証することは、既存のプロトコルにとって無理のない拡張である。モバイルクライアントおよびアクセスルータの認証に検出メカニズムを用いることにより、プロトコル信号数を大幅に節約できる。プロトコル信号数の節約は、通信資源が貴重かつ高価であるモバイル無線ネットワークにとって重要である。検出メカニズムを用いるさらなる利点は、検出メカニズムがIPv4およびIPv6両方に共通であることである。従って、検出メカニズムをキャリアとして用い、モバイルクライアントおよびアクセスルータの認証を実行する本発明は、ネットワークがIPv4とIPv6とのいずれを用いるかにかかわらず、ネットワークにおいて実行可能である。

【0009】本発明にかかる認証プロトコルは、AAAインフラストラクチャに基づいて、AAAプロトコルにより提供される認証サービスおよびプロトコル信号を用いてもよい。AAAプロトコルにおいては、複数のドメインが定められ、各ドメインは少なくとも1つのAAAサーバにより管理される。AAAサーバは、アテンダント、すなわちアクセスルータを介してモバイルクライアントに対しAAAサービスを提供する。本発明では、請求メッセージに含まれるクライアントの身元証明書を確認するために、信用できる実体が必要である。クライアントが新たなフォーリンドメインに入った場合、信用できる実体は、クライアントのホームドメインを管理するAAAサーバである。従って、この最初の認証過程のためにプロトコル信号がクライアントとホームサーバとの間を往復するため、通信の待ち時間を生じるかもしれない。しかしながら、クライアントがフォーリンドメインにとどまっている限りにおいて、ホームサーバは確認のために用いられない。例えば、クライアントがフォーリンドメイン内でアクセスルータを切り替えた場合は、こ

のフォーリンドメインのサーバが信用できる実体になる。クライアントが同一のアクセスルータに接続を要求する場合、そのアクセスルータでさえも信用できる実体になってよい。従って、本発明にかかる認証プロトコルに必要なプロトコル信号は、より短い距離を往復することにより、認証プロセスにより生じる通信の遅延が短縮化される。

【0010】本発明にかかる認証プロトコルは、対称および非対称鍵暗号方式等のいかなる鍵アルゴリズムを用いても実行可能である。これらの鍵は、本発明の認証過程に伴うプロトコル信号とともに配信されてもよい。これらの鍵が配信されることにより、2つの実体間に新たなセキュリティ関係が確立され、アドレス解決(ARP/RARP)等の近隣検出や実体間の以後の通信のためのプロトコル信号を安全にする。

【0011】本発明の別の実施形態においては、アクセスルータは、自らの身元証明書を含む通知メッセージを自発的に送信してもよい。この身元証明書を正常に確認した場合、クライアントは、このアクセスルータをインターネットへのゲートウェイとして使用する。この証明を確認できない場合には、自らの身元証明書を含む請求メッセージを送信することにより、認証過程を開始する。この請求メッセージは、上記で概説したように処理される。

【0012】本発明の別の実施形態においては、クライアントは、アクセスルータと通信中に、このアクセスルータに対し請求メッセージを送信してもよい。通信中でさえも、正当な実体が不正な実体と入れ替わる可能性は常にある。この請求メッセージを受けて、アクセスルータが自らの身元証明書を含む通知メッセージを送信し、よって、クライアントは通信中にアクセスルータを再認証できる。同様に、アクセスルータは、通信中のクライアントに対し有効期間の短い通知メッセージを送信してもよい。この通知メッセージに対し、クライアントは自らの身元証明書を含む請求メッセージを送信し、よって、アクセスルータはクライアントを再認証できる。

【0013】クライアントからの請求メッセージおよび/またはアクセスルータからの通知メッセージがチャレンジを含み、リプレイ攻撃から防御してもよい。

【0014】

【発明の実施の形態】ここで、本発明の好適な実施形態を図面を参照しつつ説明する。この図面において、同様の構成要素には同一の参照符号が付される。本明細書に記載されている実施形態は、性質上、例示的なものすぎず、本発明の範囲を限定するものではない。なお、本実施形態中に記載のネットワークでは、モバイルIPが用いられているが、本発明は、より広く、IPv4およびIPv6等のいかなるIPベースの通信プロトコルを用いても実行可能である。

【0015】図1に、本発明が適用される第3世代の無

線モバイルアクセスIPに対応したデータ通信ネットワーク100を示す。本明細書の目的のため、データ通信ネットワーク100は、無線移動体通信ネットワークに関するIMT-2000規格およびITUの仕様に従うものとする。さらに、データ通信ネットワーク100は、IETFで提案されているモバイルIPv4およびモバイルIPv6規格に従い、モバイルIP支援を実行するものとする。したがって、勿論、本願では、一方のバージョンに特有の用語を他方のバージョンの対応する用語に置き換えて使用してもよい。例えば、「エージェント」という用語は、「アクセスルータ」や、単に「ルータ」という用語に置き換えて使用してもよい。同様に、「エージェント検出」は、「ルータ検出」と、「エージェント請求」は、「ルータ請求」と、「登録要求」は、「対応更新」と、それぞれ置き換えて使用してもよい。

【0016】無線モバイルアクセスIPに対応したデータ通信ネットワーク100の中心には、多数の図示せぬ固定ノード、すなわち固定接続ポイントまたはリンクを有する固定ノードIPデータネットワークであるコアネットワーク120が備えられている。この通信ネットワーク内またはこの通信ネットワークを介し、また、インターネットプロトコルバージョン6(IPv6)に従い、デジタルデータの送受信がなされる。上述したように、IPv6は通信プロトコルのほんの一例でありIPv4等の通信プロトコルと置き換えることが可能である。コアネットワーク120のいくつかのノードは、図示せぬ従来のルータを有し、このルータは、従来のインターネットアドレッシングおよびルーティングプロトコルに従って中間ノードとして機能し、ネットワークに接続された送信元および送信先ノード間でデータパケットを転送する。

【0017】コアネットワーク120には、複数のゲートウェイルータ(GR)130が備えられており、これらがIPモバイルバックボーンを構成している。このIPモバイルバックボーンを構成するゲートウェイルータ130は、それ自体がコアネットワーク120のノードであり、コアネットワーク120を介して相互接続されている。各ゲートウェイ130には、モバイルクライアント135と通信可能な複数のアクセスルータ145が接続されている。このモバイルクライアントとしては、コードレス電話機、携帯電話機、携帯型コンピュータ、個人情報管理機器等の種類の異なるモバイル無線通信装置が利用可能である。アクセスルータ145は、ホームルータ(HR)およびフォーリンルータ(FR)として機能し、ゲートウェイルータ130を介してクライアント135をコアネットワーク120に接続する。アクセスルータ145は、アクセスネットワークのレイヤ3上の実体である。クライアント135は、無線アクセスポイント(AP)155を介してアクセスルータ145と

通信する。このAP155は、アクセスネットワークのレイヤ2上の実体である。一群のAP155は、図1のサブネットワーク150を構成している。各アクセスルータ145は、サブネットワーク150を管理し、サブネットワーク150とデータネットワーク100との間のインターフェースとしてネットワークリンクを提供する。クライアント135およびAPは、周知のCDMA、W-CDMA、または同様なデジタルデータ通信技術を用い、互いに通信する。

【0018】モバイルIPv6に従い、各クライアント135には、ホームルータであるアクセスルータ145を含むホームサブネットワークが割り当てられる。このアクセスルータ145は、クライアント135の現在位置情報を保持し、クライアント135の現在位置にパケットを転送する。その他のアクセスルータ145は、フォーリンルータとして機能する。クライアント135は、ホームサブネットワークから離れている間、このフォーリンルータに「訪問する」ことができる。クライアント135が、任意の時刻にホームルータあるいはフォーリンルータのいずれかと通信する場合、いずれかのルータがネットワークリンクを確立し、クライアント135にネットワークアクセスを提供する。ネットワーク上のクライアント135およびアクセスルータ145は、従来のインターネットプロトコルを用いた従来の固定ノードデータネットワークと同様に、それぞれ一意のIPアドレスをもつ。

【0019】データ通信ネットワーク100全体の中で、2つのレベルのハンドオフ過程が考えられる。第1のレベルは、マクロレベルハンドオフまたはレイヤ3ハンドオフであり、クライアントの位置の変化をとともなう。この位置の変化とは、クライアントが、あるアクセスルータにより管理される無線サブネットワークから、別のアクセスルータにより管理される無線サブネットワークに移動することである。従って、L3ハンドオフにより、クライアントのネットワークリンクは必然的に変化する。第2のレベルは、マイクロレベルハンドオフまたはレイヤ2ハンドオフであり、サブネットワーク150内でのクライアントの位置変化をとともなう。この場合、クライアントの無線リンクは変化するが、ネットワークリンクは変化しない。L2ハンドオフ処理は、無線携帯通信ネットワークにおいて一般的である。例えば、隣接するAPからのビーコン信号の強度を用いて隣接するAPの到達可能性を検出することは周知である。

【0020】図2は、モバイルIPv6に従って行われるモバイルクライアントによるL3ハンドオフ過程を示す簡略図である。図2において、データ通信ネットワーク100は、コアネットワーク120およびコアネットワーク120に接続されるアクセスルータ145を含む。クライアント135は、初めは出発点Aに位置し、中間地点Bを経由して地点Cに移動する。図2におい

て、出発点Aのクライアント135は、フォーリンルータであるアクセスルータ145 (FR1) に管理されるフォーリンサブネットワーク内で動作し、FR1を介してコアネットワーク120に接続されている。一方、地点Cは、フォーリンルータであるアクセスルータ145 (FR2) に管理されるフォーリンサブネットワーク内に位置している。モバイルクライアント135は、FR1に管理されるサブネットワークを通り抜け、FR2に管理されるサブネットワークに入る。従って、図2において考えられるL3ハンドオフは、ネットワークリンクをFR1からFR2へと切り替える際に行われる。

【0021】クライアント135が、出発点Aから移動し中間地点Bに到着するとき、ある時点でFR1とのさらなる無線通信が失敗し始める。クライアント135は、FR1に管理されるサブネットワーク150を離れ、FR2に管理されるサブネットワーク150に入るところである。クライアント135が中間地点Bを通りすぎ、L2ハンドオフが行われると、クライアント135の無線リンク先は、FR1に管理されるサブネットワークのAPからFR2に管理されるサブネットワークのAPに変わる。到着地点Cに近づくにつれ、クライアント135は、L3ハンドオフ、すなわちFR2との間でモバイルIP登録をおこなう。この登録過程では、モバイルIPv6に定められるルータ検出が最初に行われる。このルータ検出により、クライアント135は隣接するアクセスルータ145を検出し、このアクセスルータ145のリンク層アドレスを特定し、このアクセスルータ145への経路についての到達可能性情報を保持する。このために、ルータ検出において、一対のICMP (Internet Control Message Protocol) パケットタイプ、すなわちルータ請求およびルータ通知が定義される。ルータ請求は、クライアントにより送信され、隣接するアクセスルータにルータ通知の生成および返信を要求するメッセージである。アクセスルータ145は、定期的またはクライアント135からのルータ請求に対して、ルータ通知を送信することにより、自らの存在を通知する。ルータ通知が含む情報に基づき、クライアント135は気付けアドレス (CoA) を設定する。

【0022】FR2からルータ通知を受信すると、クライアント135はこの通知内の情報に基づいて気付けアドレスを生成、設定する。そして、クライアント135は、新しい気付けアドレスおよびクライアント135の不変のホームIPアドレスを含む対応更新をホームルータに送信することにより、新しい気付けアドレスを登録する。ホームルータは、アドレスの対応情報を記録するキャッシュ内のクライアントのルーティング情報を更新し、その結果、クライアント135とFR2との間にL3リンクが確立される。以後、クライアント135のホームIPアドレスに送信されるパケットは、ホームルー

タにより途中で回収され、FR2にトンネル送信され、FR2からクライアント135に配信される。パケットの迂回ルーティングにより生ずるパケット遅延を解消するため、以後パケットをクライアント135に直接転送可能なあらゆる相手先ノードに対しても、対応更新が送信される。

【0023】モバイルデータ通信の人気の高まるにつれ、悪意をもったクライアントがネットワークアクセスを試みる可能性も高くなる。このクライアントは、不正IDまたは盗難IDを用いてネットワーク資源に無料でアクセスしようとする不正利用者かもしれない。ネットワークの秩序ある運用に対する脅威にほかならない。従って、この悪意をもったクライアントをふるい落とすために、ネットワークアクセスを要求するクライアントは、ネットワークアクセスが許可される前に、常に認証されなければならない。同様に、クライアントは、ネットワークアクセスを開始する前に、接続サービスを提供するアクセスルータの認証を望むかもしれない。アクセスルータの中には、クライアントの通信を盗聴したり、どこかへ転送したり、ただ中斷するだけの不正なアクセスルータがあるかもしれない。本発明が提供する双方向セキュリティプロトコルでは、クライアントおよびアクセスルータを相互に認証し、その結果、クライアントはゲートウェイとして用いる前に悪意をもったアクセスルータを特定でき、アクセスルータは転送サービスを提供する前に悪意をもったクライアントを特定できる。

【0024】本発明にかかるセキュリティメカニズムは、認証、認可、および課金 (AAA) プロトコルに基づいている。RADIUSやDIAMETER等のAAAプロトコルは、今日、インターネット上で使用されており、ダイヤルアップコンピュータに対して、認証、認可、および課金サービスを提供している。このようなAAA管理サービス、特にAAAサービスにより提供される認証サービスは、モバイルIPにおいても同様に有用である。実際、モバイルIPは、基本的な枠組みにほとんど変更を加えないAAAインフラストラクチャ上で実行可能である。例えば、AAAプロトコルにおけるクライアントは、モバイルIPのモバイルノードと考えられ、AAAプロトコルにおけるアテンダントは、モバイルIPのアクセスルータに相当する。モバイルクライアントおよびアクセスルータの機能を向上させ、これらがAAAメッセージを解読可能であれば、AAAインフラストラクチャ上でモバイルIPが実行可能になる。

【0025】図3および4は、ネットワークアクセスサービス (NAS) およびモバイルIPが実行される、一般的AAAネットワークモデルを示す簡略図である。管理ドメインは、1または共通の管理の下で動作する複数のネットワークからなる。図1に示すデータ通信ネットワーク100内において、多数の管理ドメインが定義されてもよい。しかし、図の簡略化のため、図3および4

に示すAAAネットワークには、2つの管理ドメインのみが示されている、すなわち、広域インターネットにより隔てられたホームドメイン300およびフォーリンドメイン400である。各ドメインは、ドメインの構成要素に対しAAAサービスを提供するAAAサーバを備えている。ホームドメイン300は、ホームサーバAAAH310により管理されている。フォーリンドメイン400は、フォーリンサーバAAAF410により管理されている。各ホームおよびフォーリンドメインは、ドメイン内に配置されるアテンダントをさらに備えている。ただし、図3および4では、フォーリンドメイン400のみが、2つのアテンダント420および421を備えている。AAAプロトコルに従って、アテンダント420および421は、クライアント320とローカルドメイン400との間のサービスインターフェースを提供する。この実施形態では、クライアント320は、ホームドメイン300からフォーリンドメイン400に移動し、管理ドメイン400内のアテンダント420または421のいずれかからのサービスを望んでいるものとする。上述したように、モバイルIPは、図3および4に示すAAAネットワーク上で実行される。モバイルIPの場合、アテンダントは、實際上、モバイルクライアントに対しネットワークアクセスサービスを提供するアクセスルータ（AR）である。従って、「アテンダント」という用語は、「アクセスルータ」または、単に「AR」という用語と置き換えて使用してもよい。

【0026】AAAプロトコルにより提供される重要なサービスの1つは、認証である。一般的に、AAA認証メカニズムは以下のように機能する。AAAに対応した第1の実体が通信先に望む第2の実体に対し証明書を提示し、第2の実体が第1の実体の証明書を正常に確認可能な場合のみ、2つの実体間の通信が許可される。この証明書は、2つの実体間でセキュリティ関係（SA）が確立される際に定義される鍵アルゴリズムを用いて確認される。AAAプロトコルは、異なる鍵アルゴリズムを用いても機能するように設計されている。あるアルゴリズムは、公開鍵インフラストラクチャに基づき、別のアルゴリズムは、対称鍵の配信に基づいている。AAAサーバは、鍵の配信センターとして機能し、アテンダントやクライアント等のAAAの実体の要求により、AAAの2つの実体間で提示される証明書を確認するために用いられる鍵を生成、配信する。2つのAAAの実体に対し鍵を配信することにより、これらの間にセキュリティ関係が確立される。説明上、図3および4に示すAAAネットワークでは、対称鍵または共有秘密鍵アルゴリズムが用いられるものとする。対称鍵アルゴリズムは、他の鍵アルゴリズムよりも用い易く、インターネット全体への適応性という問題に解決策を提供する。しかしながら、本発明を実施するにあたり、公開鍵方式等の非対称鍵アルゴリズムや他の鍵アルゴリズムを用いてもよいこ

とは、当業者にとっては明らかであろう。また、認証トークンを用いてもよい。

【0027】図3および4に示すAAAネットワークには、暗黙のセキュリティモデルが存在する。図5は、このような暗黙のセキュリティモデルを示しており、矢印は、初めから確立されていると想定されるセキュリティ関係を示す。まず、矢印SA1が示すように、AAAF410とAR420および421との間にセキュリティ関係が確立されているものとする。ARはAAAF410に管理されるドメインに位置しており、両者間にはすでに信用が確立されているはずであるので、AR420および421とAAAF410との間にSA1が確立されているものとしてよいであろう。次に、AAAH310とAAAF410との間にセキュリティ関係が確立されているものとする。これらのAAAサーバは、初め、両者間にセキュリティ関係を確立している必要はないが、必要に応じて両者間にセキュリティ関係を確立する能力をもたねばならない。矢印SA2が示すセキュリティ関係は、2つのAAAサーバ間で直接的に、または仲介AAAサーバ200を介して間接的に、確立可能である。最後に、矢印SA3が示すように、クライアント320とAAAH310との間にセキュリティ関係が確立されているものとする。クライアント320は、AAAH310が位置するホームドメイン300からスタートしているので、SA3が確立されているものとしてよいであろう。従って、AAAH310は、最初にクライアントを認証可能な唯一の実体である。

【0028】本発明の重要な特徴は、本発明ではルータ検出メカニズムが「キャリア」として用いられ、モバイルIPにおいてAAAセキュリティプロトコルを実行する点である。本発明では、ルータ請求およびルータ通知が拡張され、既存のAAAプロトコルにモバイルIP認証機能を付加する。

【0029】＜最初のルータ検出（新しいドメインに入る場合）＞図6は、本発明の実施形態にかかる、ルータ検出プロトコルを用いたネットワークアクセス認証過程を示すフローチャートである。図7は、図6に示す過程の簡略図である。この実施形態では、クライアント320は、AR420および421、またはAAAF410のいずれともセキュリティ関係を確立していないものとする。すなわち、クライアント320は、以前にフォーリンドメイン400に訪問したことがないか、もしくは長期間フォーリンドメイン400から離れていたためAR420、AR421、およびAAAF410との間で以前に確立されたセキュリティ関係が無効になったものとする。

【0030】クライアント320は、フォーリンドメイン400に入り、リンクが張られているアクセスルータによるネットワークアクセスを要求する。ステップ501において、クライアント320は、拡張ルータ請求メ

ッセージ(RS+)を送信することによりルータ検出を開始する。これはマルチキャストメッセージであり、クライアントと同じリンク上のすべてのアクセスルータにより受信される。通常のルータ請求メッセージとは異なり、これはクライアントの身元証明書を含む。この身元証明書は、標準のルータ請求パケットの拡張という形で送信される。RS+は、標準のルータ請求メッセージ(RS)と同様の各種構成要素を含む。また、RS+は、ネットワークアクセス識別子(NAI)またはIPアドレスになりうるクライアントの識別子(client_id)と、クライアントの署名とを含む。この署名は、AAAH310と共有するクライアントの秘密鍵(client-AAAH_key)により暗号化されたRS+の要約である。従って、RS+は以下のように表現される。

RS + client_id + クライアントによる署名

【0031】クライアントの共有秘密鍵は、クライアント320とAAAH310との間に確立されるセキュリティ関係SA3(図5参照)により定義される。従って、AAAH310は、クライアントの共有秘密鍵(client-AAAH_key)を保有し、RS+に格納されたクライアントの署名を確認する。AR420および他のアテンダントは、クライアント320からRS+を受信する。しかしながら、上述したように、AR420はクライアント320とセキュリティ関係を確立していないため、クライアント320の身元を確認する共有秘密鍵を保有しない。標準のルータ検出メカニズムによると、アクセスルータはルータ請求メッセージに応じてルータ通知メッセージを返信する。しかしながら、本発明では、クライアント320が正常に認証されるまで、AR320および他のアクセスルータはルータ通知メッセージを返信しない。

【0032】AR420は、クライアント320の確認をAAAF410に委任する。AR420は、AAA要求メッセージ(AAAReq)を生成し、AAAF410に送信する(ステップ503)。このAAAReqは、クライアント320からのRS+全体のコピーを含む。AR420からAAAF410へ送信されたAAAReqは、両者間に確立されたセキュリティ関係SA1に基づいて保護される。AAAReqは、RadiusやDIAMETER等のAAAプロトコルに従って生成される。AAAメッセージを生成する際の好適な手順については、「Diameter基本プロトコル」と題されたIETFの草案「draft-ietf-diameter-07.txt」および「DiameterモバイルIP拡張仕様」と題されたIETFの草案「draft-calhoun-diameter-mobileip-12.txt」の中で論じられている。なお、この2つの草案は本明細書において参照として援用

される。

【0033】上述したように、AAAF410は、クライアント320とセキュリティ関係を確立しておらず、従って、クライアントの身元を確認する共有秘密鍵を保有していない。しかし、RS+に格納されたクライアントの識別子により、AAAF410はクライアント320のホームドメインがホームドメイン300であることを認識する。そして、AAAF410は、AAAH310との間に確立されたセキュリティ関係SA2を使って、ホームドメイン300に位置するAAAH310に対しRS+のコピーとAAAReqを転送する(ステップ505)。

【0034】AAAF410からAAAReqを受信すると、AAAH310は、クライアントの共有秘密鍵を用いてAAAReqに格納されたクライアントの署名を復号することにより、クライアント320の身元を確認する。クライアントが正当な身元を提示すれば、AAAH310はクライアントの身元を正常に確認できるはずである。クライアントの身元を確認できない場合、AAAH310はAAA応答メッセージ(AAARep)を生成し、AAAF410を介してAR420に送信する。このAAARepは、AAAH310がクライアント320を認証できない旨を示す認証結果を含む。AAARepも、RadiusやDIAMETER等のAAAプロトコルに従って生成される。AAARepを受信すると、AR420はクライアント320からのルータ請求メッセージを無視し、ルータ通知メッセージを返信しない。従って、認証されないクライアントによるネットワーク資源へのアクセスは防止される。

【0035】AAAH310がクライアント320の身元を正常に確認した場合、AAAH310は、AAA応答(AAARep)を生成しAAAF410に送信することにより、AAAF410からのAAAReqに応答する(ステップ507)。このAAARepは、2つの共有秘密鍵を含む。これらのうち一方は、クライアント320とAR420との間で用いられ、他方は、クライアント320とAAAF410との間で用いられる。これらの共有秘密鍵はAAAH310により生成され、AAAF410、AR420、およびクライアント320に配信され、クライアント320とAAAF410との間およびクライアント320とAR420との間にセキュリティ関係を確立する。これらの共有秘密鍵である(client-AR_key)および(client-AAAF_key)は、それぞれ複製される。複製された共有秘密鍵(client-AR_key)および(client-AAAF_key)は、これらの真実性および機密性を守るため、クライアント320と共有する秘密鍵(client-AAAF_key)を用いてAAAF410により暗号化され、クライアント320に配信される。元の鍵(client-AR_key

y) および (client - AAAF_key) は復号化され、AR420 および AAAF410 にそれぞれ配信される。従って、AAAH310 から AAAF410 に送信される AAARep は、以下のように表現される。

client - AR_key + client - AAAF_key + AAAH により暗号化された (client - AR_key + client - AAAF_key)

【0036】AAAH310 からの AAARep により、AAAF410 はクライアント320 が信用できることを認識する。そして、AAAF410 は、AAARep から復号化された共有秘密鍵 (client - AAAF_key) を抽出し、キャッシュに格納する。この抽出された共有秘密鍵は、クライアント320 からのメッセージを認証するため、AAAF410 により用いられる。そして、AAAF410 は、AAARep を AR420 に転送する (ステップ509)。AAAF410 からの AAARep により、AR420 はクライアント320 の身元が正常に認証されたことを認識する。そして、AR420 は、AAARep から復号化された共有秘密鍵 (client - AR_key) を抽出し、キャッシュに格納する。この共有秘密鍵は、クライアント320 からのメッセージを認証するため、AR420 により用いられる。そして、AR420 は、拡張ルータ通知 (RA+) を生成し、クライアント320 に送信する (ステップ511)。この RA+ は、標準のルータ通知メッセージ (RA)、AR420 の識別子 (AR_id)、および共有秘密鍵 (client - AAAF_key) により暗号化された共有秘密鍵 (client - AR_key) および (client - AAAF_key) を含む。この RA+ は、さらに AR420 の署名を含む。この署名は、AR420 が AAAF410 から受信した共有秘密鍵 (client - AR_key) により暗号化された RA+ の要約である。従って、この RA+ は以下のように表現される。

RA + AR_id + AAAH により暗号化された (client - AR_key + client - AAAF_key) + AR による署名

【0037】AR420 から RA+ を受信すると、クライアント320 は受信した RA+ を認証する。まず、クライアント320 は、AAAH310 と共有する秘密鍵 (client - AAAH_key) を用いて、共有秘密鍵 (client - AR_key) および (client - AAAF_key) を復号化する。これらの秘密鍵が正常に復号化された場合、これらの鍵はクライアント320 が信用する AAAH310 により証明されることから、クライアント320 はこれらの秘密鍵を信用できる。次に、クライアント320 は、復号化された秘密鍵 (client - AR_key) を用いて、AR420

の署名を復号化する。署名が正常に復号化された場合、AR420 の身元はクライアント320 が信用する秘密鍵 (client - AR_key) により確認されることから、クライアント320 は AR420 を信用できる。また、署名が正常に復号化されることにより、クライアント320 に対し RA+ の信頼性が保証される。クライアント320 および AR420 に配信される共有秘密鍵 (client - AR_key) により、クライアント320 と AR420 との間に新しいセキュリティ関係 SA4 (図8参照) が確立される。クライアント320 および AAAF410 に配信される共有秘密鍵 (client - AAAF_key) により、クライアント320 と AAAF410 との間に新しいセキュリティ関係 SA5 が確立される。

【0038】AR420 の署名を認証できない場合、クライアント320 は AR420 からの RA+ を無視し、認証可能な証明書を含む他のアクセスルータからの RA+ を待つ。従って、クライアント320 が不正なアクセスルータを介してネットワークアクセスを開始してしまうことを防止できる。

【0039】図6および7に示す認証過程は、長時間を要し、かなりの通信待ち時間を生じるであろう。この通信待ち時間は、主に AAA メッセージが AAAF410 と AAAH310 とを隔てる広域インターネットを行き来するために要する時間である。AAA メッセージが AAAF410 あるいは AAAH310 に送信される場合、常に、いくらかの待ち時間を伴う。図6および7に示す最初の認証過程では、これら遠く離れたサーバと通信しなければならない。しかしながら、もし AR420 および AAAF410 が AAAF410 あるいは AAAH310 によらずにクライアントを認証できれば、認証メカニズムに伴う待ち時間が短縮化される。

【0040】<以降のルータ検出 (同一ドメイン内で、新しいアクセスルータを検出する場合) > クライアント320 は、ドメイン400 内を移動し、クライアント320 の身元を認証していない別のアクセスルータと接続してもよい。図9は、本発明の別の実施形態に基づき、このような場合に行われる認証ルータ検出を示すフローチャートである。図10は、図9に示す過程の簡略図である。図9および10において、図6および7に示す AR420 との最初の認証過程を経た後、クライアント320 は、AR420 に管理されるサブネットワークを離れ、AR421 に管理されるサブネットワークに入るものとする。AR421 を介してネットワークにアクセスするため、クライアント320 は RS+ を再び送信する (ステップ701)。今回送信される RS+ は、図6および7に示す最初の認証過程で用いられたものと同様のメッセージを含み、以下のように表現される。

RS + client_id + クライアントによる署名

【0041】しかしながら、本実施形態のRS+に含まれる署名は、共有鍵 (client - AAAF_key) により暗号化されるため、AR421は署名を確認することができない。そこで、AR421は、AAAReqを生成しAAAF410に送信することにより、クライアント320の確認をAAAF410に委任する (ステップ703)。AR421からのAAAReqは、RS+全体のコピーを含む。AAAF410は、図6および7に示す先の認証過程において共有秘密鍵 (client - AAAF_key) を取得しているため、クライアント320の身元を認識できるはずである。AAAF410は、AAAH310によることなく、共有秘密鍵 (client - AAAF_key) でクライアント320の署名を復号化することにより、クライアント320の身元を確認する。クライアント320の署名を確認できない場合、AAAF410は、AAAReqを生成し、AR421に送信する (ステップ705)。これにより、AR421に対し、クライアント320が信用できない旨を知らせる。AR421は、クライアント320からのRS+を無視する。クライアント320の署名が正常に確認された場合、AAAF410は、クライアント320とAR421との間で共有する秘密鍵 (client - AR2_key) を生成する。この秘密鍵 (client - AR2_key) は、複製される。複製により2つとなった秘密鍵の一方はそのまま暗号化されず、他方は共有秘密鍵 (client - AAAF_key) により暗号化される。AAAF410は、暗号化されていない鍵と暗号化された鍵とをAAAReqに格納し、AR421に送信する (ステップ705)。従って、AAAF410からAR421に送信されるAAAREpは、以下のように表現される。
client - AR2_key + AAAFにより暗号化された (client - AR2_key)

【0042】AAAF410からのAAAREpにより、AR421はクライアント320が信用できることを認識する。そして、AR421は復号化された秘密鍵 (client - AR2_key) を抽出し、キャッシュに格納する。この格納された秘密鍵は、クライアント320からの以後のメッセージを認証するため、AR421により用いられる。AR421は、RA+を生成し、クライアント320に送信する (ステップ707)。AR421からのRA+は、以下のように表現される。

RA + AR_id + AAAFにより暗号化された (client - AR2_key) + ARによる署名

【0043】AR421からRA+を受信すると、クライアント320は、共有秘密鍵 (client - AAAF_key) を用いて復号化し、秘密鍵 (client - AR2_key) を抽出する。もしこの鍵が正常に復

号化されたら、クライアント320はこの鍵を信用できる。クライアント320は、共有秘密鍵 (client - AR2_key) を用いてAR421の署名を復号化することにより、RA+を認証する。署名が正常に復号化された場合、クライアント320はAR421およびRA+の真実性を信用できる。クライアント320およびAR421に配信される共有秘密鍵 (client - AR2_key) により、両者間に新しいセキュリティ関係が確立される。署名を復号化できない場合、クライアントはAR421からのRA+を無視し、認証可能な署名を含む他のアクセスルータからのRA+を待つ。

【0044】図9および10に示す、以降の認証過程は、図6および7に示す認証過程と比較して迅速に行われる。これは、図9および10に示す認証過程では、AAAH310とメッセージをやり取りする必要がなく、従って、プロトコル信号がより短い距離を往復するためである。

【0045】＜以降のルータ検出 (同一アクセスルータを検出する場合)＞各RA+には、有効期間がある。従って、同一のアクセスルータに接続している場合でも、先のRA+の有効期間が経過する前に、クライアントは同一のアクセスルータとの認証過程を経なければならない。この場合、図11および12に示すように、本発明にかかる認証過程において、プロトコル信号は最短距離を往復する。図11および12では、クライアント320は、ステップ801においてRS+をAR420に送信する。RS+は、以下のように表現される。

RS + client_id + クライアントによる署名

【0046】署名は、図6および7に示す最初の認証過程においてクライアント320が取得した共有秘密鍵 (client - AR_key) により暗号化される。AR420は、クライアント320と同一の鍵を共有しているため、クライアント320の身元を認識できるはずである。AR420は、AAAF410によらずに、共有秘密鍵 (client - AR_key) を用いて署名を復号化することにより、クライアント320の身元を確認する。クライアント320の身元を確認できない場合、AR420はRS+を無視する。クライアント320の身元を正常に確認した場合、AR420は、RA+を生成し、クライアント320に送信する。本実施形態のRA+は、以下のように表現される。

RA + AR_id + ARによる署名

【0047】従って、クライアント320とAR420との通信は、プロトコル信号が最短距離を往復するため最速の認証メカニズムである。

【0048】＜非請求ルータ通知＞アクセスルータは、認証可能なRS+の受信を待つのではなく、RA+を定期的に送信してもよい。図13において、AR420および421はRA+を定期的に送信するものとする。R

A+は、以下のように表現される。

RA + AR_id + ARによる署名

【0049】AR420から送信されるRA+は、RAとAR420の署名とを含む。AR421から送信されるRA+は、RAとAR421の署名とを含む。クライアント320は、図6および7に示すAR420との最初の認証過程を以前に経ているものとする。先の認証過程を通じて、クライアント320とAR420との間、およびクライアント320とAAAF410との間には、セキュリティ関係が確立されている。AR420からのRA+がクライアント320に到達していれば、クライアント320はRA+を認証できるはずである。従って、クライアント320は、AR420を介して安全にネットワークアクセスを開始できる。受信するいかなるRA+も認識できない場合、クライアントは、RS+を送信することにより、図6および7に示す最初の認証過程を経なければならない。

【0050】<再認証>通信中のクライアントおよびARのどちらも常に、本発明の認証過程を開始し、互いに再認証してよい。これは、通信中でさえも悪意をもった実体が正当な実体と入れ替わる可能性が常にあるという理由から重要である。クライアントは、ARとの通信中、RS+を送信することにより、いつでもこの過程を開始してよい。ARは、クライアントによる再認証に対しRA+をクライアントに返信することにより、RS+に回答できるはずである。同様に、ARは、クライアントを収容している間、クライアントを再認証できる。ARは、有効期間の非常に短いユニキャストルータ通知メッセージをクライアントに送信することにより、クライアントの再認証を開始する。このルータ通知メッセージは有効期間が非常に短いことから、クライアントは、ARがまもなくクライアントへの接続サービスを停止することを認識する。クライアントは、RS+を送信し同一リンク上の利用可能な他のアクセスルータを検出することにより、このようなルータ通知メッセージに回答する。そして、ARは、クライアントから送信されたRS+を認証する。

【0051】<旧プロトコルとの相互運用>ネットワーク全体において、本発明にかかる拡張ルータ検出メカニズムをサポートできるドメインと、標準のルータ検出メカニズムのみをサポートできるドメインとが混在してもよい。従って、標準のルータ検出メカニズムのみをサポートするクライアントが、本発明にかかる拡張ルータ検出メカニズムをサポートするドメインに移動する場合があってもよいし、また、拡張ルータ検出メカニズムをサポートするクライアントが、標準のルータ検出メカニズムのみをサポートするドメインに移動する場合があってもよい。どちらの場合も、本発明にかかる認証プロトコルは、標準のルータ検出メカニズムの運用の妨げとはならない。

【0052】まず、拡張ルータ検出メカニズムをサポートするクライアントが、標準のルータ検出メカニズムのみをサポートするドメイン内において接続サービスを受けようとする場合、クライアントはRS+を送信する。しかしながら、隣接するアクセスルータは、RS+に加えられた新しい拡張部分を認識できず、従って、この拡張部分を無視する。アクセスルータは、RS+をrとして処理し、RAを返信する。ここで、この「認証されていない」ルータ通知メッセージを用いるか否かはクライアント次第である。

【0053】次に、標準のルータ検出メカニズムのみをサポートするクライアントが、本発明にかかる拡張ルータ検出メカニズムをサポートするドメイン内において接続サービスを受けようとする場合、クライアントは、いかなる新しい拡張をも含まないRSを送信する。このような「認証されない」ルータ請求メッセージを受信した場合、RA+を返信するか、あるいは全く応答しないかは、隣接するアクセスルータ次第である。

【0054】どちらの場合であっても、本発明にかかる拡張ルータ検出メカニズムをサポートするクライアントおよびARは、通信相手が拡張ルータ検出メカニズムをサポートできるか、または標準のルータ検出メカニズムのみをサポートできるのかを検出し、それに応じて応答できる。認証されていないメッセージに対し応答するか、または受け取るかは、ネットワークの設計方針次第である。

【0055】<リプレイ攻撃に対する防御>リプレイ攻撃とは、盗難パスワードの単なる再利用である。パスワード送信中にクラッカーがそのパスワードを盗聴できれば、クラッカーはそれ以降いつでも使用できるパスワードのコピーを手に入れることになる。たとえパスワードが暗号化されてやり取りされていたとしても、クラッカーは、以前に取得した通信を単に再実行することにより、ログインできるかもしれない。本発明にかかる認証プロトコルは、チャレンジに関する拡張を加えることにより、リプレイ攻撃に対する防御を設けることができる。

【0056】図14は、チャレンジ方式を用いてリプレイ攻撃に対する防御を設ける本発明の実施形態を示すフローチャートである。図14においては、クライアント320は、AR420またはAAAF410と通信することがなく、従って、図6および7に示す最初の認証過程を経なければならないものとする。まず、クライアント320は、RSを送信する(ステップ1001)。AR420は、RSを受信するが、RSを送信したクライアントの身元が認証されるまで信用できない。RSを送信したクライアントは、クライアント320との過去の通信を盗聴し、クライアント320の識別情報を盗み、偽造IDを使ってネットワークにアクセスする悪意をもったノードかもしれない。

【0057】クライアント320からのRSに対する返信として、AR420は、クライアントの身元およびRSの真実性を確認する（ステップ1003）。具体的には、ステップ1003において、AR420は、チャレンジに関する拡張とRAをクライアント320に送信する。このチャレンジに関する拡張は、AR420により生成された乱数を含む。AR420からのRAをきっかけとして、クライアント320は、拡張ルータ請求メッセージ（RS*）を生成、送信する（ステップ1005）。RS*は、RSと、クライアントの識別子、すなわちクライアントのIPアドレスまたはNAIと、秘密鍵の要求とを含む。この秘密鍵は、AR420と共有され、AR420とのセキュリティ関係を確立する。RS*は、さらに2つのチャレンジに関する拡張を含む。一方のチャレンジに関する拡張は、ステップ1003においてクライアントがAR420から受信したチャレンジのコピーを含み、他方のチャレンジに関する拡張は、クライアント自身により生成された乱数を含む。最後に、RS*は、クライアント320とAAAH310との間で共有される秘密鍵（client-AAAH_key）を用いて暗号化されるクライアント320の署名を含んだ認証拡張を含む。従って、本実施形態において、RS*は以下のように表現される。

RS + client_id + client-AR_key_request + Chal_AR + Chal_client + クライアントによる署名

【0058】クライアント320からRS*を受信すると、AR420は、チャレンジに関する拡張（Chal_AR）をチェックし、この拡張に含まれる乱数がステップ1003においてクライアントに送信した乱数と同一であるかを調べる。乱数が同一の場合、RS*は、事実上、ステップ1003においてAR420がクライアント320に送信したチャレンジに対する応答であるといえる。乱数が一致しない場合、おそらくRS*は、盗難IDを使ってクライアント320だと偽る悪意をもったノードからのものであるため、AR420はこのRS*を無視しなければならない。乱数が一致した場合、以降の認証過程は、図6および7において述べた過程と同様である。

【0059】クライアント320の身元がAAAH310により正常に確認された場合、AR420は、拡張ルータ通知メッセージ（RA*）を生成し、クライアント320に対し送信する（ステップ1007）。本実施形態において、RA*は、RAと、クライアント320とAR420との間で共有する秘密鍵（client-AR_key）とを含む。この秘密鍵は、AAAH310により生成されたものである。上述したように、この鍵は、クライアント320とAAAH310との間で共有する秘密鍵（client-AAAH_key）を用いて暗号化される。RAは、さらに2つのチャレンジに関

する拡張を含む。一方のチャレンジに関する拡張は、ステップ1005においてAR420がクライアントから受信した乱数のコピーを含み、他方のチャレンジに関する拡張は、AR420により生成されクライアント320とAR420との間の次の通信で用いられる新しい乱数を含む。RA*は、新しく配信された共有秘密鍵（client-AR_key）を用いて暗号化されたAR420の署名を含んだ認証拡張も含む。従って、本実施形態のRA*は、以下のように表現される。

RA + AR_id+client-AR_key_reply + Chal_client + Chal_AR + ARによる署名

【0060】AR420からRA*を受信すると、クライアント320は、チャレンジに関する拡張（Chal_client）をチェックし、この拡張に含まれる乱数がステップ1005においてAR420に送信した乱数と同一であるかを調べる。乱数が一致しない場合、悪意をもったアクセスルータが盗難IDを使ってAR420だと偽っているかもしれないため、クライアント320はこのRA*を無視しなければならない。乱数が一致した場合、クライアント320は、チャレンジに関する拡張（Chal_AR）から乱数を抽出し、AR420との以後の通信のためキャッシュに格納する。そして、クライアント320は、AAAH310と共有する秘密鍵（client-AAAH_key）を用いて鍵応答（client-AR_key_reply）を復号化し、AR420と共有する秘密鍵（client-AR_key）を抽出する。この抽出された共有秘密鍵を用いて、クライアントはAR420の署名を確認する。

【0061】図14に示す最初の認証過程を実行後、すなわちクライアント320とAR420との間でセキュリティ関係が確立された後、クライアント320およびAR420は、互いに再認証してもよい。図15に、このような再認証過程の一例を示す。再認証過程において、まず、クライアント320がRS*を送信する（ステップ1101）。これに対する返信として、AR420は、RA*を送信する（ステップ1103）。クライアント320とAR420との間でセキュリティ関係が既に確立されているので、RS*は以下のように表現される。

RS + client_id + Chal_AR + Chal_client + クライアントによる署名

【0062】RS*のチャレンジに関する拡張（Chal_AR）は、ステップ1007においてコピーされた乱数を含む。チャレンジに関する拡張（Chal_client）は、クライアントにより生成された新しい乱数を含む。

【0063】RA*は、以下のように表現される。

RA + AR_id + Chal_client +

Chal_AR + ARによる署名

【0064】RA*のチャレンジに関する拡張(Chal_client)は、ステップ1101においてコピーされた乱数を含む。チャレンジに関する拡張(Chal_AR)は、ARにより生成された新しい乱数を含む。

【0065】＜非対称鍵方式を用いた認証＞上述した実施形態においては、対称鍵方式、すなわち共有秘密鍵アルゴリズムを用いるAAAインフラストラクチャに基づいた、本発明にかかる認証プロトコルについて説明した。本発明にかかる認証プロトコルが公開鍵アルゴリズム等の非対称鍵方式を採用しても機能することは、当業者にとって明らかである。図16を参照して、いかに本発明にかかる認証プロトコルが公開鍵アルゴリズムを用いて機能するかについて説明する。図16において、クライアント320が以前に訪問したことのないドメイン400に入ったものとする。従って、クライアント320は、最初の認証過程を経なければならない。

(1) クライアント320は、RS+を送信することにより、ルータ検出を開始する。本実施形態において、RS+は、RSを含む。また、RS+は、クライアント320の識別子とクライアント320の署名とを含む。この署名は、クライアント320の秘密鍵を用いて暗号化されたRS+の要約である。従って、RS+は、以下のように表現される。

RS + client_id + クライアントによる署名

【0066】クライアント320の秘密鍵は、クライアント320とAAAH310との間に確立されるセキュリティ関係SA3(図5参照)により定義される。従って、AAAH310は、クライアント320の公開鍵を保有し、RS+に格納されたクライアント320の証明書を確認する。図16に示す設定では、AAAH310が、クライアントの署名を確認できる唯一の実体である。

(2) AR420は、クライアント320からRS+を受信するが、クライアント320の署名を復号化する公開鍵を保有しないため、署名を確認できない。そこで、AR420は、AAAREqを生成し、RS+全体のコピーとともにAAAF410に送信する。

(3) AAAF410は、クライアント320の公開鍵を保有せず、クライアント320の署名を確認できない。そこで、AAAF410は、自身の公開鍵をAAAREqに格納し、AAAH310に転送する。

(4) AAAF410からAAAREqを受信すると、AAAH310は、クライアント320の公開鍵を用いてAAAREqに格納されたクライアント320の署名を復号化することにより、クライアント320の身元を確認する。クライアント320の署名を正常に確認した場合、AAAH310は、AAAREpを生成しAAAF410に送信することにより、AAAREqに

AAAREpに回答する。このAAAREpは、クライアント320の公開鍵(PK)とAAAF410の証明書とを含む。AAAF410の証明書は、AAAREqからAAAF410の公開鍵を抽出し、これを暗号化することにより生成される。なお、暗号化する際、既に確立されたセキュリティ関係SA3により定義されるAAAH310の秘密鍵が用いられる。従って、AAAH310からAAAF410に送信されるAAAREpは、以下のように表現される。

クライアントのPK + AAAHにより証明されたAAAF

(5) AAAF410は、AAAREqからクライアント320の公開鍵を抽出し、キャッシュに格納する。この抽出された公開鍵は、クライアント320からのメッセージを認証するために、AAAF410により用いられる。AAAF410は、AR420の証明書を生成し、AAAREpにこの証明書を格納し、AAAREpをAR420に送信する。AR420の証明書は、AAAF410の秘密鍵により証明されたAR420の公開鍵(PK)を含む。従って、AAAF410からAR420に送信されるAAAREpは、以下のように表現される。クライアントのPK + AAAFにより証明されたAR + AAAHにより証明されたAAAF

(6) AAAF410からAAAREpを受信すると、AR420は、クライアント320の公開鍵を抽出し、キャッシュに格納する。クライアント320の公開鍵は、クライアント320からのメッセージを認証するために、AR420により用いられる。AR420は、RA+を生成し、クライアント320に送信する。このRA+は、RAと、AAAF410により生成されたAR420の証明書と、AAAH310により生成されたAAAF410の証明書とを含む。従って、RA+は、以下のように表現される。

RA + AR_id + AAAFにより証明されたAR + AAAHにより証明されたAAAF + ARによる署名

【0067】AR420からRA+を受信すると、クライアント320は、受信したRA+を認証する。クライアント320は、まずAAAH310の公開鍵を用いてAAAF410の証明書を復号化し、AAAF410の公開鍵を抽出する。この公開鍵は、クライアント320とAAAH310との間に確立されているセキュリティ関係SA3に由来する。証明書が正常に復号化された場合、クライアント320は抽出されたAAAF410の公開鍵を信用できる。これは、この鍵がクライアント320が信用するAAAH310により証明されたためである。次に、クライアント320は、抽出されたAAAF410の公開鍵を用いてAR420の証明書を復号化し、AR420の公開鍵を抽出する。証明書が正常に復

号化された場合、クライアント 320 は、AR420 の公開鍵を信用できる。これは、この鍵がクライアント 320 が信用する AAAF410 により証明されたためである。クライアント 320 に配信された AR420 および AAAF410 の公開鍵を用いて、クライアント 320 と AR420 との間およびクライアント 320 と AAAF410 との間に新しいセキュリティ関係 SA4 および SA5 (図 8 参照) が確立される。

【0068】以上本発明の好適な実施形態を説明してきたが、これらは、性質上、例示的なものにすぎず、本発明の範囲を限定するものではない。本発明の斬新かつ有利な特徴を保ちつつ、且つ本発明の趣旨を逸脱せずに、種々の変形および追加を加えてもよいことは、当業者にとって明らかである。従って、本発明の範囲は、正しく解釈された添付の請求の範囲によってのみ定義される。

【0069】

【発明の効果】以上説明したように、本発明によれば、クライアントとアクセスルータとが相互に認証することにより、不正なクライアントまたは不正なアクセスルータによる通信を防止できる。また、本発明によれば、ネットワーク層において認証メカニズムが実行されるため適用可能なアクセス技術が限定されない。さらに、本発明は、既存の通信プロトコルにおいて広く用いられているルータ検出が認証プロトコルのキャリアとして用いられるので、既存の通信プロトコルへの導入が容易である。

【図面の簡単な説明】

【図 1】 本発明が適用される第 3 世代の無線移動体アクセス IP に対応するデータ通信ネットワークの一例を示す図である。

【図 2】 図 1 に示すデータ通信ネットワークにおいて行われる標準的なモバイルクライアントによる L3 ハンドオフ処理を示す簡略図である。

【図 3】 本発明にかかる認証プロトコルが実行される一般的な AAA ネットワークモデルを示す簡略図である。

【図 4】 本発明にかかる認証プロトコルが実行される一般的な AAA ネットワークモデルを示す簡略図である。

【図 5】 図 3 および 4 に示すネットワークにおいて、既に確立されている暗黙のセキュリティモデルを示す図である。

【図 6】 モバイルクライアントの身元がホームサーバにより確認される本発明の実施形態にかかる、ルータ検

出メカニズムを用いた認証プロトコルを示すフローチャートである。

【図 7】 図 6 に示す過程の簡略図である。

【図 8】 図 6 および 7 に示す認証プロトコル実施後、クライアントとアクセスルータとの間 (SA4) およびクライアントと AAAF との間 (SA5) に確立される新しいセキュリティ関係を示す図である。

【図 9】 モバイルクライアントの身元がフォーリンサーバにより確認される本発明の別の実施形態にかかる、認証プロトコルを示すフローチャートである。

【図 10】 図 9 に示す過程の簡略図である。

【図 11】 クライアントおよびアクセスルータが再認証される本発明の別の実施形態にかかる、認証プロトコルを示すフローチャートである。

【図 12】 図 11 に示す過程の簡略図である。

【図 13】 アクセスルータがルータ通知を自ら送信する本発明の別の実施形態を示す簡略図である。

【図 14】 請求および通知メッセージがチャレンジを含みリプレイ攻撃に対し防御を設ける本発明の実施形態にかかる、ルータ検出メカニズムを用いた認証プロトコルを示すフローチャートである。

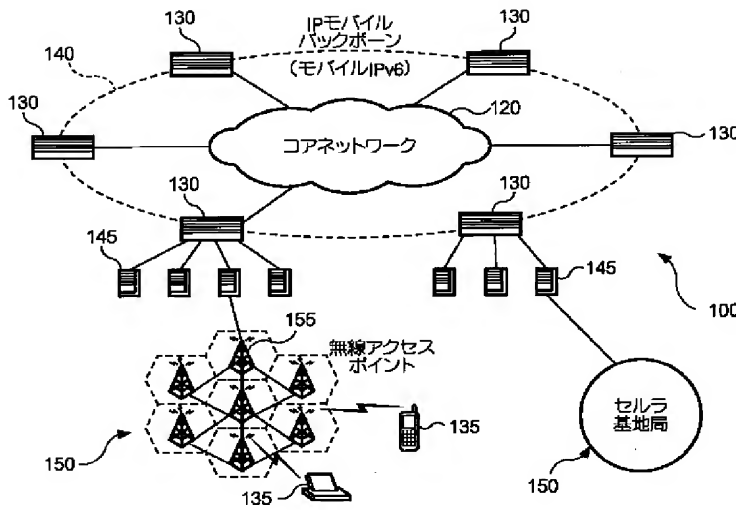
【図 15】 クライアントおよびアクセスルータが再認証される、図 14 に示す本発明の実施形態において行われる認証プロトコルの別の例である。

【図 16】 非対称鍵アルゴリズムが用いられる本発明の実施形態にかかる、ルータ検出メカニズムを用いた認証プロトコルを示すフローチャートである。

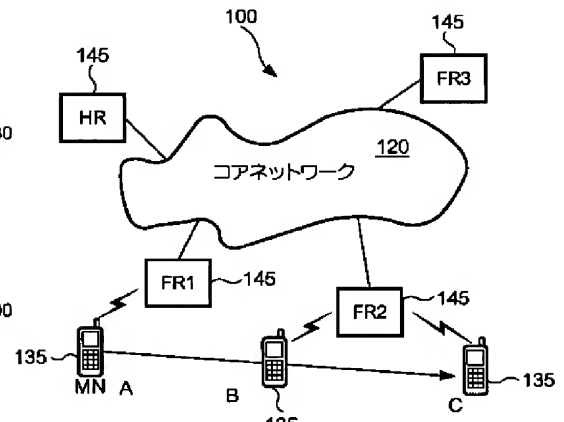
【符号の説明】

100 データ通信ネットワーク
120 コアネットワーク
130 ゲートウェイルータ
135、320 クライアント
140 IP モバイルバックボーン
145、420、421 アクセスルータ
150 サブネットワーク
155 無線アクセスポイント
200 仲介サーバ
300 ホームドメイン
310 ホームサーバ
400 フォーリンドメイン
410 フォーリンサーバ

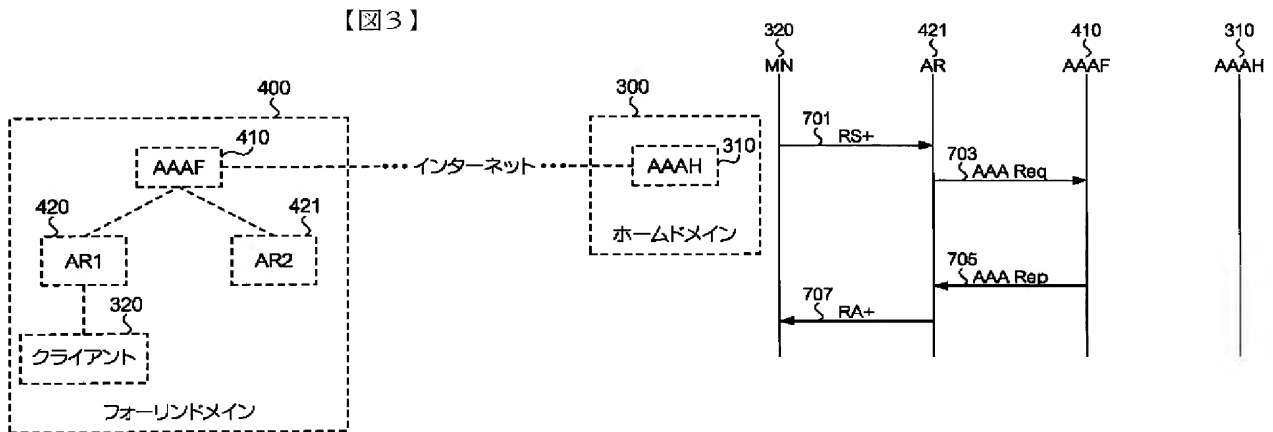
【図 1】



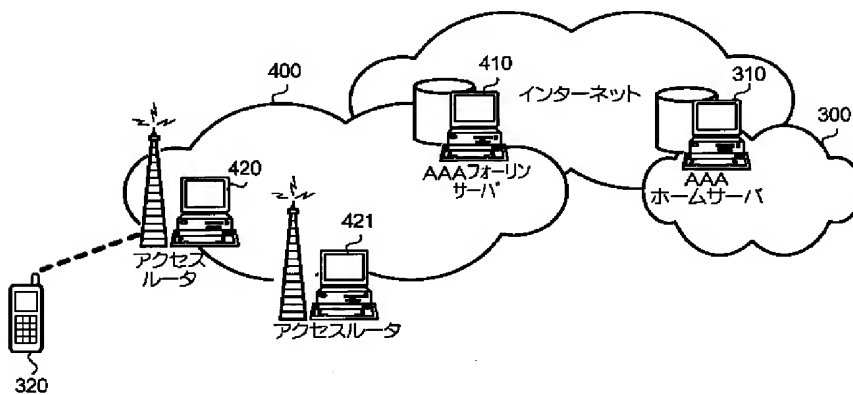
【図 2】



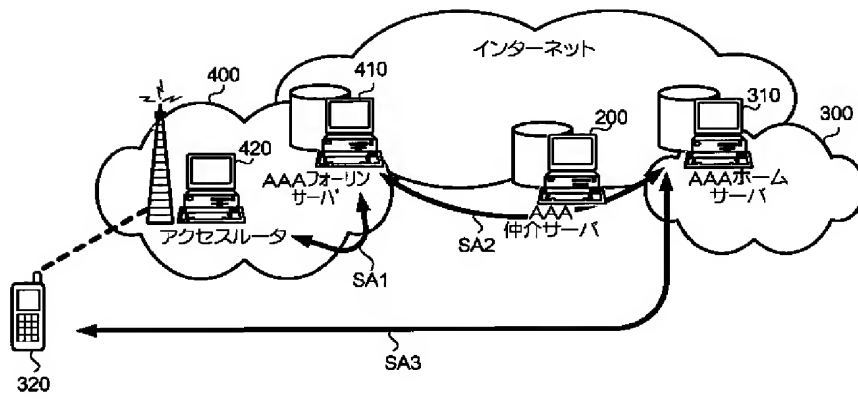
【図 9】



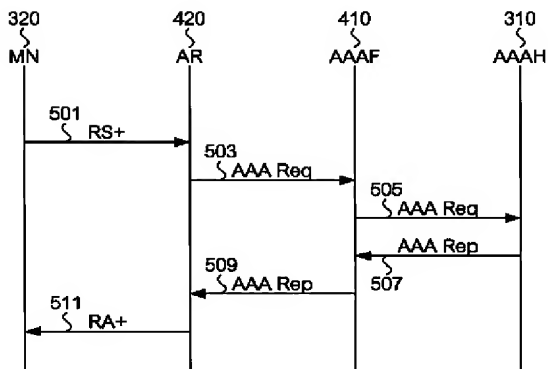
【図 4】



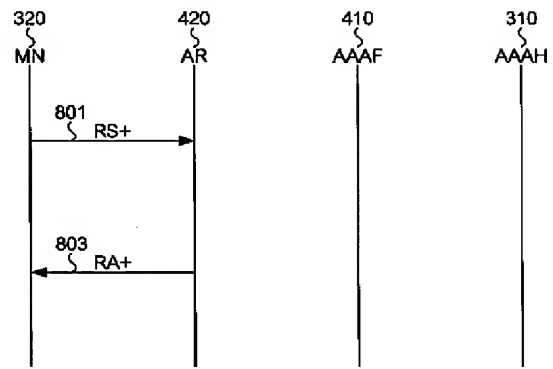
【図5】



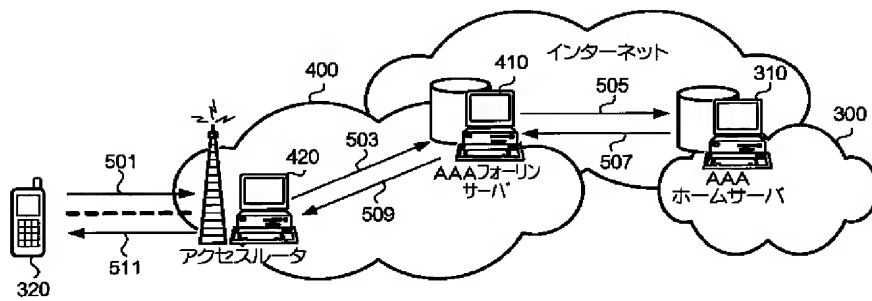
【図6】



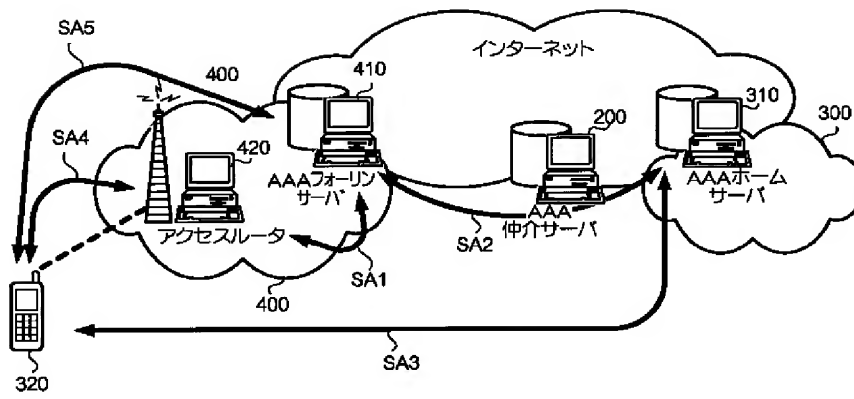
【図11】



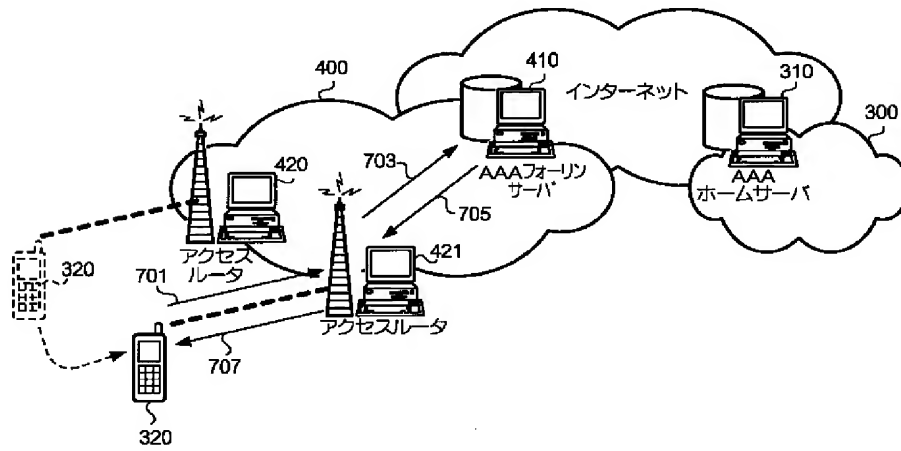
【図7】



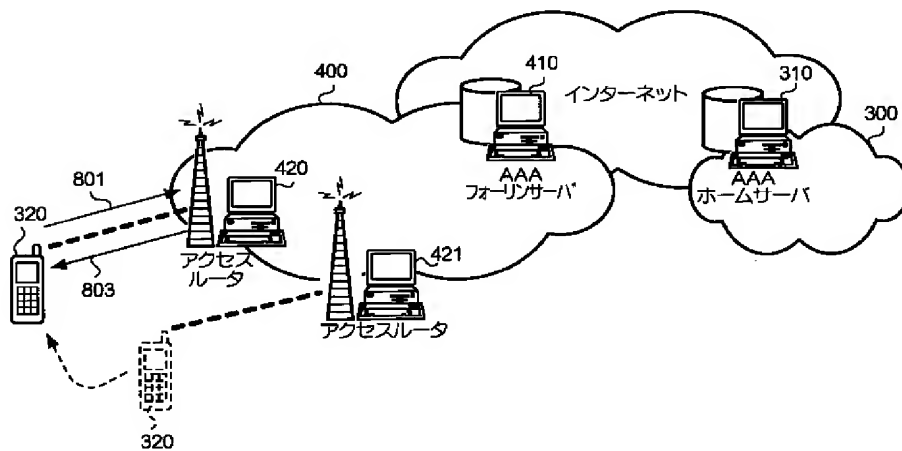
【図8】



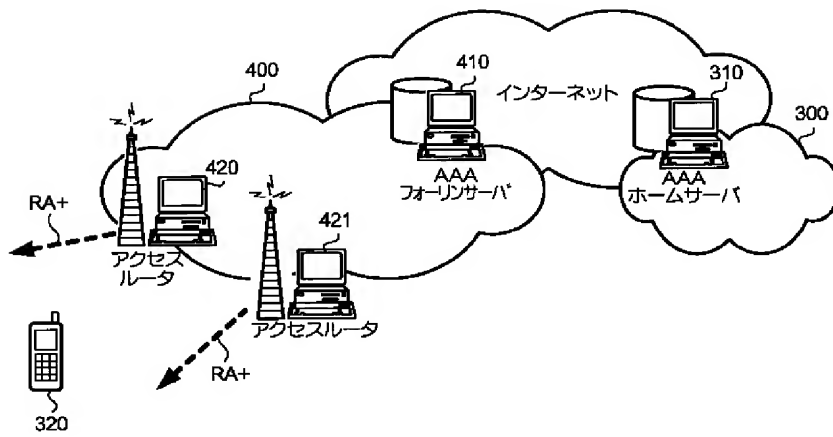
【図10】



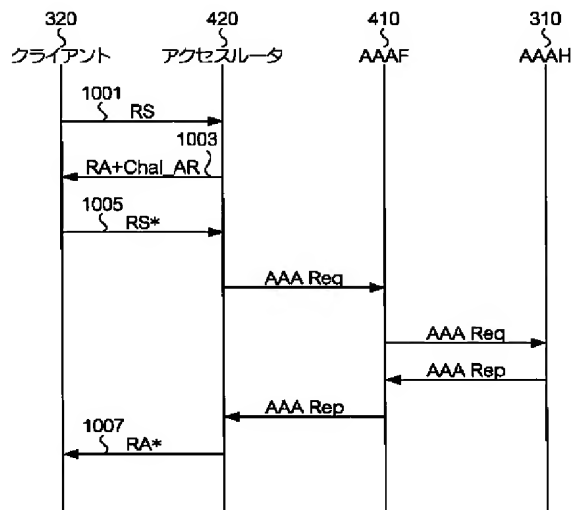
【図12】



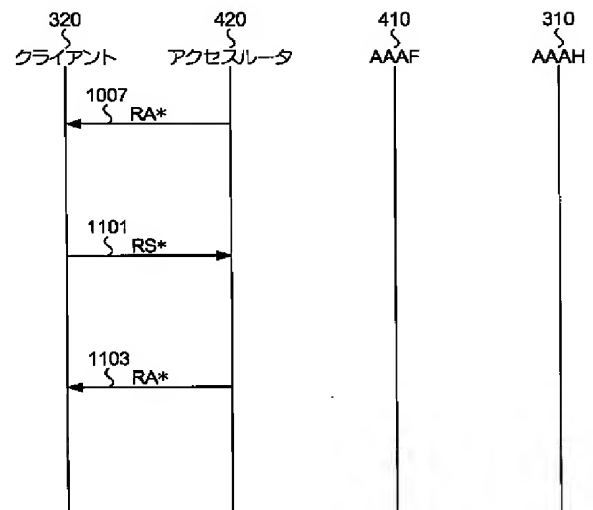
【図13】



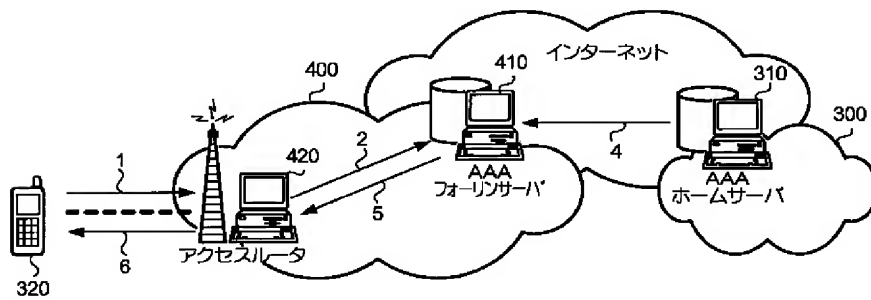
【図14】



【図15】



【図16】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	キーワード (参考)
H 0 4 Q	7/24 7/26 7/30		
(72)発明者	アルパー イー ヤイン アメリカ合衆国、カリフォルニア州 94404、フォスターシティ、#シー、フォ スターシティ ブールバード 1033	(72)発明者	カール ウィリアムス アメリカ合衆国、カリフォルニア州 94306、パロ アルト、#154、エル カミ ノ ロード 3790
(72)発明者	ジョンニン ハ アメリカ合衆国、カリフォルニア州 94087、サニーベイル、#5701、ウエスト エル カミノ ロード 250	Fターム(参考)	5J104 AA07 KA04 KA05 MA01 PA02 PA07 5K030 GA15 HA08 HC01 HC09 HD03 LC13 5K033 AA08 DA01 DA06 DA19 DB18 5K067 AA21 BB04 BB21 DD11 DD51 EE02 EE10 EE16 FF02 HH11 HH22